CSCE604243 Kriptografi & Keamanan Informasi

Semester Genap 2019/2020

Informasi Umum

- Pengajar: Amril Syalim, Ph.D.
- Referensi:
    1. William Stallings. Cryptography and network security: principles and practice. Pearson; 2017.
    2. Nigel Smart. Cryptography: An Introduction (http://people.cs.bris.ac.uk/~nigel/Crypto_Book/)
- Prasyarat: Matematika Diskret I, Matematika Diskret II, Statistika dan Probabilitas, Jaringan Komputer
- Kredit: 4SKS
- Web: https://scele.cs.ui.ac.id/course/view.php?id=832, key: CSCE604243

Tujuan

Mata kuliah ini mengajarkan dasar-dasar kriptografi modern. Setelah mengikuti matakuliah ini, mahasiswa memahami teknik-teknik kriptografi modern antara lain: kriptografi simetrik, kriptografi asimetrik, fungsi hash, tanda-tangan digital, dan protokol keamanan.

Evaluasi

Komposisi penilaian (total 105%) terdiri dari:

- 30% UTS
- 30% UAS
- 15% Quiz/Latihan/Kehadiran
- 30% Tugas perkelompok

Rencana Pengajaran

Minggu	Topik	Keterangan
1	00-Math Background 1	
2	00-Math Background 2	
3	00-Math Background 3	
4	00-Math Background 4	
5	01-Classical Ciphers	Presentasi topik 1
6	02-DES	Presentasi topik 2
7	03-AES and review	
8	UTS	Jadwal ditentukan fakultas
9	04-Mode of Operations	Presentasi topik 3
10	05-Hash Function	Presentasi topik 4

11	06-Public Key Cryptography and RSA	Presentasi topik 5
12	07-Digital Signatures: RSA and DSA	Presentasi topik 6
13	08-Diffie-Hellman Key Exchange and PRNG	Presentasi topik 7
14	09-Protocol: PGP	Presentasi topik 8
15	Review	
16	UAS	Jadwal ditentukan fakultas